Microsoft Windows 2000 Server

Operating System

Configuring Enterprise Security Policies

Beta 3 Technical Walkthrough

Abstract

The integration of the Security Configuration Tool Set with the Group Policy infrastructure allows you to configure security policies for domains and organizational units contained in the Active Directory™directory services in a Microsoft® Windows® 2000-based operating system network.

This walkthrough builds on information contained in the “Using the Security Configuration Tool Set” technical walkthrough, which describes how to configure local security policies on individual computers. You might find it useful to read that walkthrough before performing this one, which describes how to configure security policies at the enterprise level.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0799

CONTENTS

INTRODUCTION

The walkthrough entitled “Using the Security Configuration Tool Set” describes how to configure local security policies on individual computers. This walkthrough describes how to use the same technology to define security policies for domains and organization units (OUs) in the Active Directory™ directory services. This functionality is enabled by the integration of the Security Configuration Tool Set with the Group Policy infrastructure. In short, the Security Configuration Tool Set extends the Group Policy infrastructure, which allows you to establish security policies within Group Policy Objects (GPOs). These GPOs are then assigned to the domain or organizational unit scope in the Active Directory, so that they can be applied to all computers in that scope, thus propagating these security policies to all computers in the domain or OU that the GPO is associated with.

Group policy is one of the key change and configuration management technologies provided in the Microsoft® Windows® 2000 operating system. Administrators use Group Policy to specify options for managed desktop configurations for groups of computers and users. This paper examines the Group Policy options for security settings. (For more information on Group Policy and Windows Administration, see http://www.microsoft.com/windows.)

The Security Configuration Tool Set is a set of Microsoft Management Console (MMC) tools designed to simplify, integrate, and centralize security configuration and analysis tasks for systems running the Microsoft Windows NT® and Windows 2000 operating systems. MMC provides a common environment for snap-ins, which define a management behavior. Snap-ins are administrative components integrated into the MMC interface. The Security Configuration Tool Set is a set of snap-ins for MMC that is designed to provide a central repository for security-related administrative tasks. (For more information, see the “Security Configuration Tool Set” white paper.)

Walkthrough Overview

This walkthrough describes how security policies can be enforced on multiple computers in your enterprise. (For configuring local security policies on individual computers, consult the walkthrough entitled “Using the Security Configuration Tool Set.”)

Before configuring Group Policy Objects (GPOs) with security settings, you can examine the Security Policy Configuration Overview section, which includes useful information about the security policies and tools you will be using, as well as some guidelines for working with GPOs. The walkthrough then addresses the following tasks:

- Viewing domain security policies
- Viewing domain controller security policies
- Allowing administrators to add workstations to the domain
- Enabling auditing on domain controllers

- Establishing a logon message for all computers in the domain
- Viewing a domain controller's effective security policy
- Enforcing a remote access security policy

These procedures take different paths to accomplish similar objectives, which allows you to compare different techniques for performing common tasks.

Setup

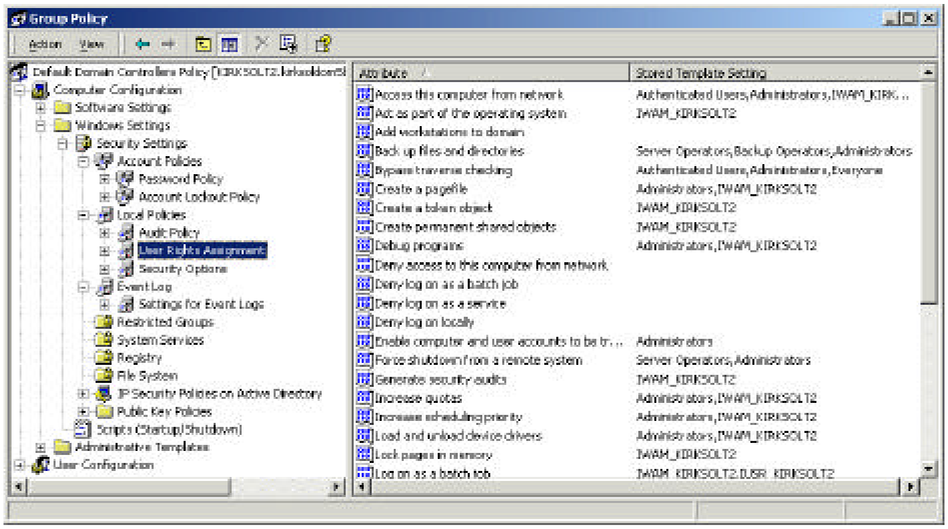
To complete these scenarios, you must log on as an administrator to a Windows 2000 domain controller.

SECURITY POLICY CONFIGURATION OVERVIEW

Security policy is defined as a security configuration file that is stored as part of a Group Policy object. This security configuration file is identical to the one used everywhere else in the tool set. You create these files using the Security Configuration Tool Set. The graphical user interface (GUI) for this tool set is provided as a set of Microsoft Management Console (MMC) snap-ins, some of which you will use in this walkthrough to configure security policies in your domains and OUs.

Security configuration for a system is subdivided into security areas. Before performing the walkthrough, you can review the security areas supported by the Group Policy framework.

Security Policies Included in the Group Policy Framework



Attribute	Stored Template Setting
Access this computer from network	Authenticated Users,Administrators,IWAM_KIRK...
Act as part of the operating system	IWAM_KIRKSOLT2
Add workstations to domain	
Back up files and directories	Server Operators,Backup Operators,Administrators
Bypass traverse checking	Authenticated Users,Administrators,Everyone
Create a pagefile	Administrators,IWAM_KIRKSOLT2
Create a token object	IWAM_KIRKSOLT2
Create permanent shared objects	IWAM_KIRKSOLT2
Debug programs	Administrators,IWAM_KIRKSOLT2
Deny access to this computer from network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Enable computer and user accounts to be tr...	Administrators
Force shutdown from a remote system	Server Operators,Administrators
Generate security audits	IWAM_KIRKSOLT2
Increase quotas	Administrators,IWAM_KIRKSOLT2
Increase scheduling priority	Administrators,IWAM_KIRKSOLT2
Load and unload device drivers	Administrators,IWAM_KIRKSOLT2
Lock pages in memory	IWAM_KIRKSOLT2
Log on as a batch job	IWAM_KIRKSOLT2,IUSR_KIRKSOLT2

Figure 1. Security Policies

- **Account Policies**—In this area, you can configure policies that apply to user accounts. This includes password policies, account lockout policies, and Kerberos policies. Password and lockout policies can be configured on member workstations and servers because workstations and servers have their own local accounts database. Kerberos policies do not apply to these local account databases, and thus make sense only on domain controller machines.
- **Local Policies**—Here you can configure local audit policy, user rights, and various security options (such as security-relevant registry values) that can be configured on a Windows 2000 system.
- **Restricted Groups**—You can establish policy regarding membership in security sensitive groups. Security sensitive groups typically include built-in groups such as Administrators and Server Operators that have privileged access to system resources by default. Additional groups can be included whenever they are considered security sensitive.
- **System Services** —You can configure security settings for system services.

Services can be configured as start-up options or you can set access control on these services.

- **Registry**—You can configure access permissions on registry keys.
- **File System**—You can configure access permissions for file system objects (folders and files).
- **Public Key Policies**—In this area, you can configure encrypted data recovery agents for Encrypting File System (EFS), domain-wide root certificate authorities, trusted certificate authorities, and so forth. This document does not include walkthroughs for configuring policies in this section. For EFS-related policies, please refer to the EFS walkthrough. For all other public key policies, refer to the public key walkthroughs.
- **IPSec Policy**—Here you can configure Internet Protocol Security (IPSec) for computers in the given scope. This document does not cover IPSec policy configurations. Please refer to the IPSec walkthroughs to learn how you can configure these policies.

The Group Policy framework supports per-computer and per-user policy settings. However, the Security Settings extension to Group Policy (described in this walkthrough) applies to computers only. You cannot configure these security settings on a per-user basis. Certain security policies, such as public key policies, can be enforced on a per-user basis. These are covered in the public key walkthroughs.

Order of Precedence for Security Policies

In this walkthrough, it is important to note the order of precedence for security policies associated with Active Directory domains and OUs, because they take precedence over policies established at the local level. The default order of precedence for security policies associated with Active Directory domains and OUs is the same as that for Group Policy in general. From the lowest to highest precedence, the ranking order is as follows:

- Local Policy
- Domain Policy
- OU Policy

Local Policy (policy defined on the computer itself) has the least precedence and the policy associated with the OU directly containing the computer has the highest precedence. (Please refer to the Group Policy walkthroughs for information on creating exceptions to this rule.)

Therefore, policies from the domain take precedence over locally defined policies. This is important to note because it can result in behavior quite different from the behavior observed in previous versions of Windows NT. For example, when password policies are configured for the Domain OU (as they are by default), those password policies are set for every computer in that domain. This means that the local account databases (on individual workstations) in the domain have the same password policy as the domain itself. In Windows NT 4.0, password policies defined for the domain did *not* impact password policies for local account databases on member workstations and servers.

Security Policy Configuration Tools

In this walkthrough, you will configure security policies using snap-ins. Snap-ins are part of the Microsoft Management Console (MMC). The Microsoft Management Console hosts tools displayed as consoles. These tools, composed of one or more applications, are built with modules called snap-ins.

You will use the following components of the Security Configuration Tool Set to configure security in this walkthrough:

- **Security Settings Extension to Group Policy**—The Security Configuration Tool Set includes an extension snap-in to the Group Policy Editor, which you will use to configure security policies for domains and organizational units.
- **Active Directory Users and Computers Snap-in**—It is a standard tool provided by Microsoft with the operating system, which you will use to perform administrative tasks.
- **Security Templates snap-in**—The Security Templates snap-in is a standalone Microsoft Management Console snap-in that allows the creation of a text-based template file that contains security settings for all security areas.

This walkthrough describes how to use these tools to view, configure, and apply security policies in domains and organizational units across your network.

Guidelines for Organizing Group Policy Objects

When working in the context of a Windows 2000 Active Directory-based enterprise, it is important to carefully organize policies to minimize redundancy and redefinition and to maximize manageability. Unfortunately, these two objectives can be at odds. To minimize redundancy and redefinition, you should try to define very granular GPOs. To maximize manageability, you should have a small number of GPOs. A small number of GPOs associated with various scopes is also essential for performance. To strike a balance, devote a reasonable amount of time to designing the layout of the policies in your infrastructure.

The steps to accomplish an organized layout include:

- Partition policies into logical groupings. For example, account policies form a logical group.
- Define one or more GPOs for each logical grouping, with different policy settings that cover possible policy values. For example, you could have one GPO that covers account policies for various domains and another one for local accounts on servers and desktops.
- Partition the computers into a hierarchical tree structure using organizational units. The partitioning should be based on the *role*—that is, the purpose or function—of each computer. For example, all domain controllers could be placed in the Domain Controllers OU by default, so that they have consistent

policies.

In general, each organization unit should map to some policy that applies to all computers in the entire OU. This can be tricky because OUs can define the corporate management hierarchy as well as the geographical layout of the organization. However, more often than not, your policy definitions will overlay your corporate and geographical layout.

When you want to apply policies to a subset of computers across your corporate organization, you can do one of the following:

- Create sub-OUs in different parts of your organization to assign the special policy to each of these sub-OUs
- If you don’t want to create deep OUs, you can use the permissions-based filtering scheme for GPOs to determine which computers a particular GPO applies to within a given OU.

CONFIGURING SECURITY POLICIES FOR ACTIVE DIRECTORY-BASED ENTERPRISES

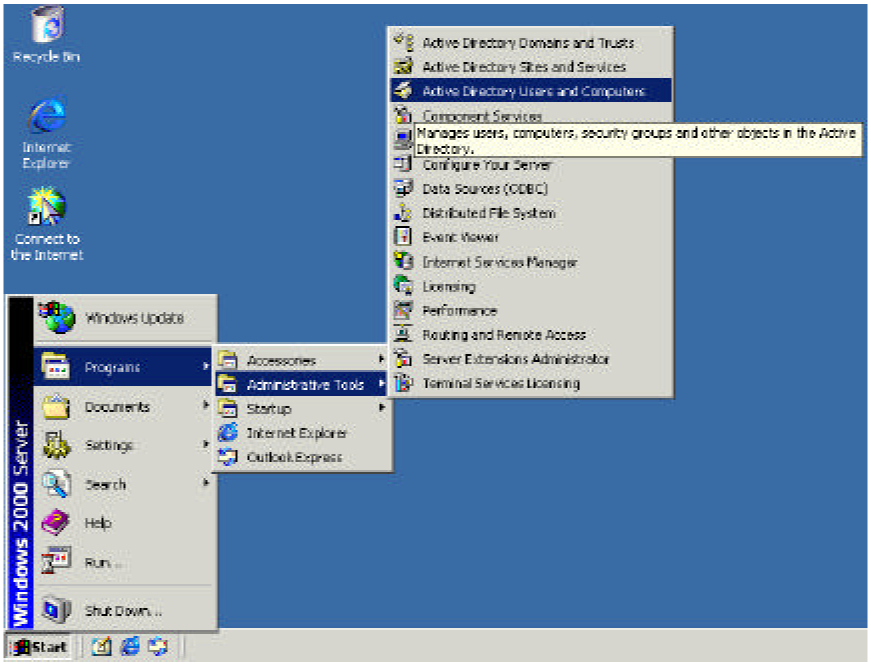
Viewing Domain Security Policies

A default domain security policy is created for each new domain. The default domain policy defines settings for the following:

- Password Policy
- Lockout Policy
- Kerberos Policy

To view domain-wide policy

1. On the **Start** menu, point to **Programs**, then point to **Administrative Tools**, and click **Active Directory Users and Computers**.



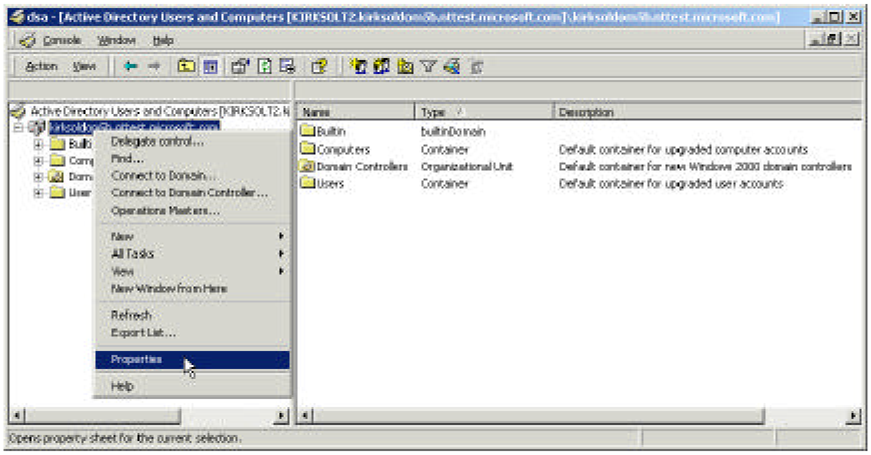
Manages users, computers, security groups and other objects in the Active Directory.

Figure 2. Adding the Active Directory Users and Computers snap-in

The **Active Directory Users and Computers** snap-in appears.

2. In the scope pane (right pane) of the snap-in, expand the domain folder to reveal the default containers. (Note that there is a Domain Controllers OU within the domain.)

3. Select the name of your domain, right-click it, and then click **Properties.** The **Properties** dialog box for your domain appears.



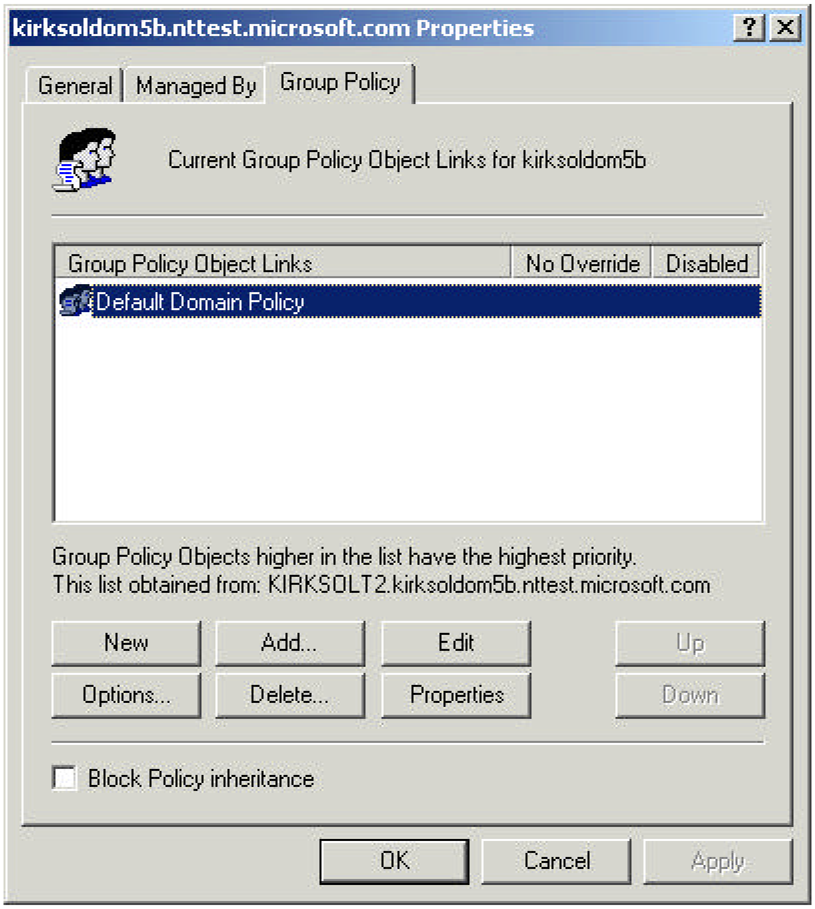
dsa - [Active Directory Users and Computers [KIRKSOLT2.kirksoldom5b.nttest.microsoft.com]\kirksoldom5b.nttest.microsoft.com]

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgraded computer accounts
Domain Controllers	Organizational Unit	Default container for new Windows 2000 domain controllers
Users	Container	Default container for upgraded user accounts

Opens property sheet for the current selection.

Figure 3. Accessing the Properties dialog box for your domain

4. Select the **Group Policy** tab, then select **Default Domain Policy**, and then click **Edit**. The **Group Policy Editor** appears.



kirksoldom5b.nttest.microsoft.com Properties

Current Group Policy Object Links for kirksoldom5b

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: KIRKSOLT2.kirksoldom5b.nttest.microsoft.com

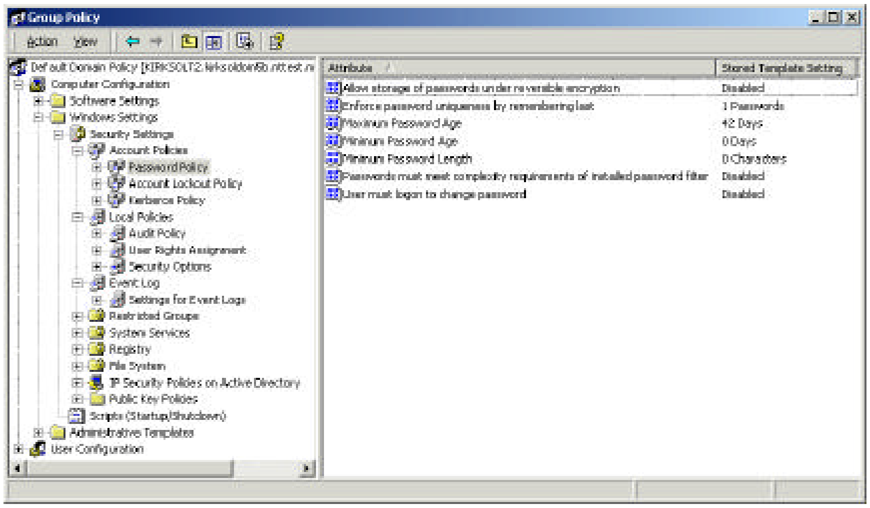
☐ Block Policy inheritance

Figure 4. Selecting the default domain policy

5. In the **Group Policy Editor**, expand **Computer Configuration**, navigate to

Windows Settings, to **Security Settings,** and then to **Account Policies**.

6. Select **Password Policy**.



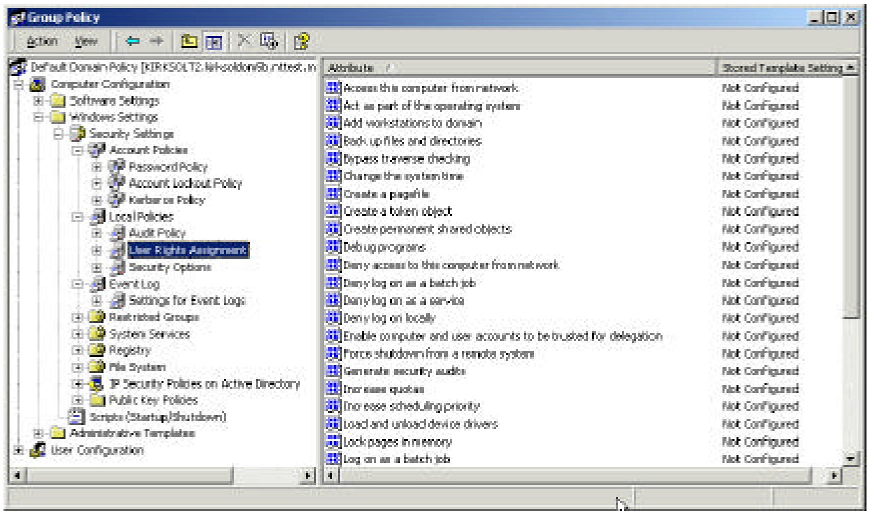
Attribute	Stored Template Setting
Allow storage of passwords under reversible encryption	Disabled
Enforce password uniqueness by remembering last	1 Passwords
Maximum Password Age	42 Days
Minimum Password Age	0 Days
Minimum Password Length	0 Characters
Passwords must meet complexity requirements of installed password filter	Disabled
User must logon to change password	Disabled

Figure 5. Viewing password policy

In the results pane, notice that **Password Policy**, **Lockout Policy**, and **Kerberos Policy** are configured by default in the domain GPO, and thus apply to all computers within that domain.

7. In the **Group Policies** dialog box, navigate from **Security Settings** to Local Policies.

8. Select the **User Rights Assignment** subfolder.



Attribute	Stored Template Setting
Access this computer from network	Not Configured
Act as part of the operating system	Not Configured
Add workstations to domain	Not Configured
Back up files and directories	Not Configured
Bypass traverse checking	Not Configured
Change the system time	Not Configured
Create a pagefile	Not Configured
Create a token object	Not Configured
Create permanent shared objects	Not Configured
Debug programs	Not Configured
Deny access to this computer from network	Not Configured
Deny log on as a batch job	Not Configured
Deny log on as a service	Not Configured
Deny log on locally	Not Configured
Enable computer and user accounts to be trusted for delegation	Not Configured
Force shutdown from a remote system	Not Configured
Generate security audits	Not Configured
Increase quotas	Not Configured
Increase scheduling priority	Not Configured
Load and unload device drivers	Not Configured
Lock pages in memory	Not Configured
Log on as a batch job	Not Configured

Figure 6. Viewing user rights assignments

Notice that none of the user rights are configured in the default domain GPO.

This does not mean that user rights are not defined for machines in your enterprise, it just means that these rights are not defined in the default domain GPO. For domain controller computers, the user rights are defined in the default domain controller GPO, which you will view next.

9. Close the **Group Policy Editor**, close the **Properties** dialog box, and then close the A**ctive Directory Users and Computers** snap-in.

Viewing Domain Controller Security Policies

In the previous section, you reviewed the domain policy configured by default for all new domains. In this section, you can review the default domain controller policy, which specifies security settings for all machines in the domain controllers OU. By default, Windows 2000 domain controller computers are added to the domain controllers OU.

In this section, you use the Group Policy snap-in rather than the Active Directory Users and Computers snap-in as the path to the default domain controller GPO.

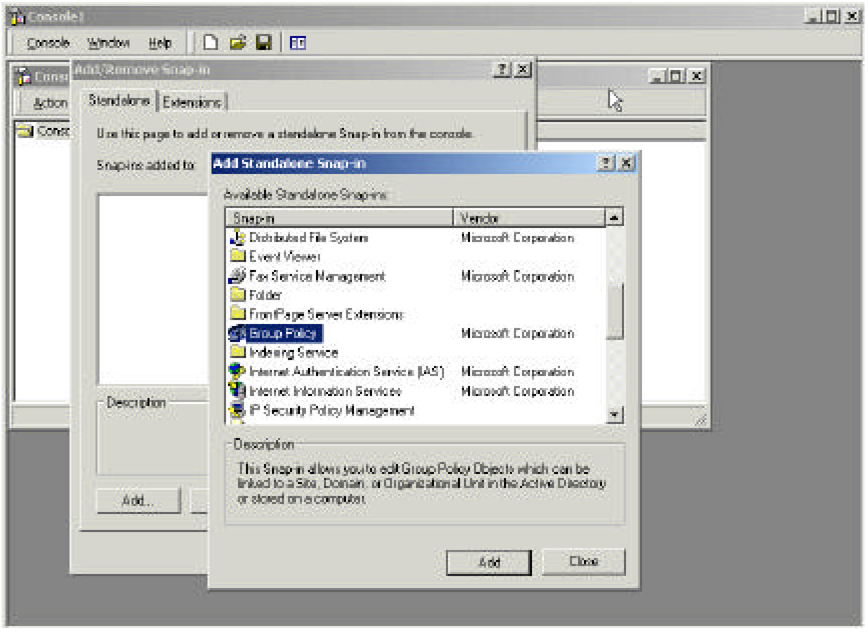
To load the Group Policy MMC snap-in

1. On the Start menu, click **Run**. In the **Open** text box, type:

   mmc/s

   and then click **OK**.

2. From the **Console** menu, select **Add/Remove Snap-in**, and click **Add**.



Use this page to add or remove a standalone Snap-in from the console.

Snap-in	Vendor
Distributed File System	Microsoft Corporation
Event Viewer	
Fax Service Management	Microsoft Corporation
Folder	
FrontPage Server Extensions	
Group Policy	Microsoft Corporation
Indexing Service	
Internet Authentication Service (IAS)	Microsoft Corporation
Internet Information Services	Microsoft Corporation
IP Security Policy Management	

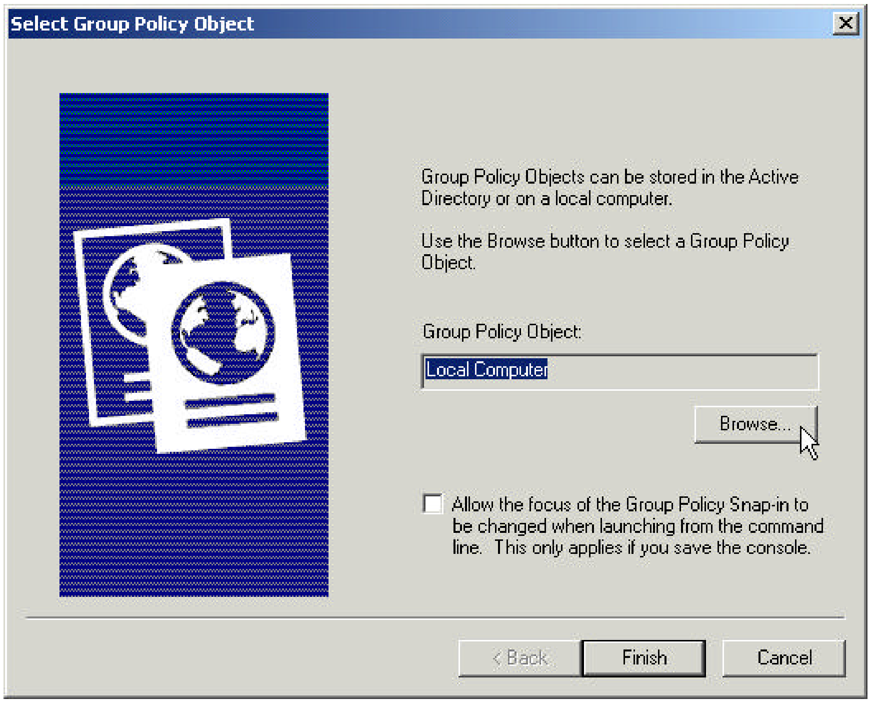
Description: This Snap-in allows you to edit Group Policy Objects which can be linked to a Site, Domain, or Organizational Unit in the Active Directory or stored on a computer.

Figure 7. Adding the Group Policy snap-in

3. From the list of available **Standalone Snap-ins**, select **Group Policy**, and click **Add**.

4. In the **Select Group Policy Object** dialog box, click **Browse**.

   The default GPO selected when the group policy snap-in is added is the one for the local computer. You want the GPO for the domain controllers OU.



Select Group Policy Object

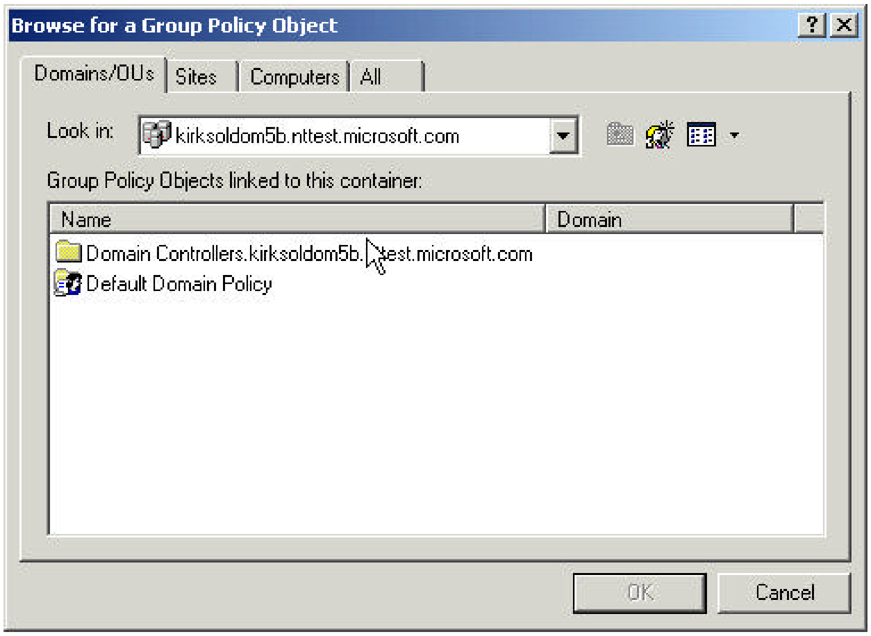
Group Policy Objects can be stored in the Active Directory or on a local computer.

Use the Browse button to select a Group Policy Object.

Group Policy Object: Local Computer

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

Figure 8. Selecting a Group Policy object



Look in: kirksoldom5b.nttest.microsoft.com

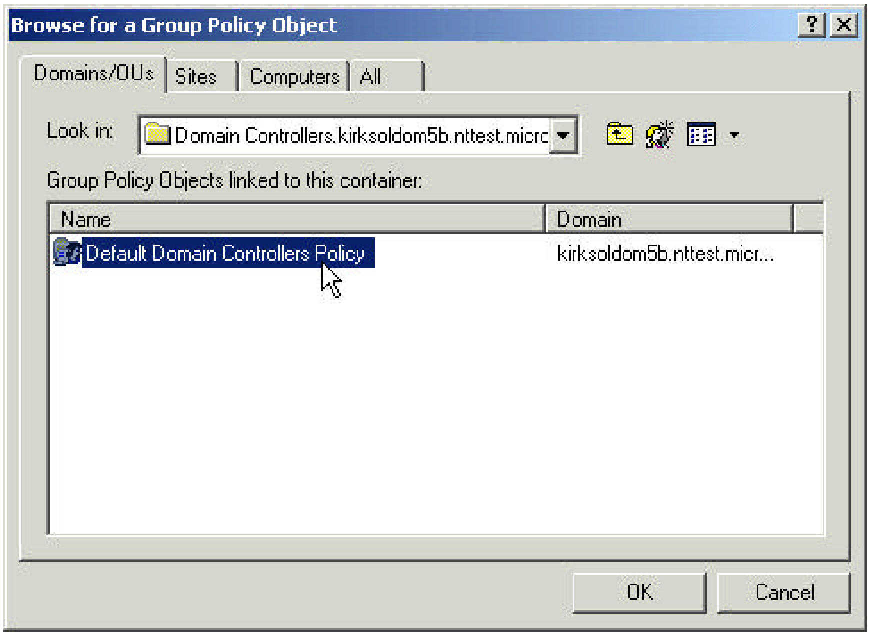
Group Policy Objects linked to this container:

Name	Domain
Domain Controllers.kirksoldom5b.nttest.microsoft.com	
Default Domain Policy	

Figure 9. Group Policy objects for a Domain Controllers OU

Note that the default domain policy (reviewed in the previous section) is also listed here, as well as a folder containing Group Policy objects for the domain controllers OU.

5. In the **Browse for a Group Policy Object** dialog box, double-click the folder containing the GPOs associated with the domain controllers OU.



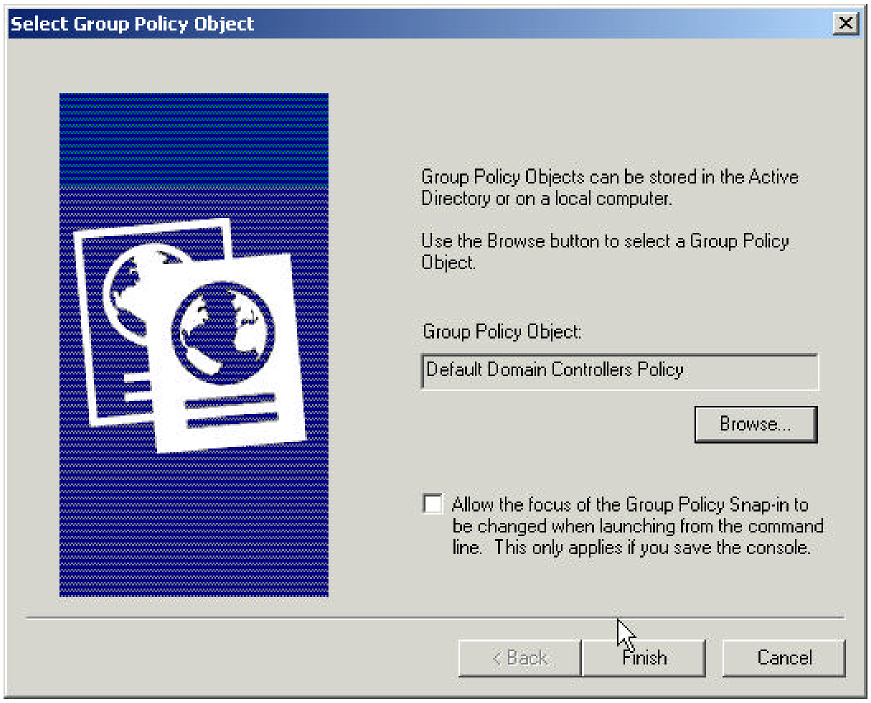
Look in: Domain Controllers.kirksoldom5b.nttest.micrc

Group Policy Objects linked to this container:

Name	Domain
Default Domain Controllers Policy	kirksoldom5b.nttest.micr...

Figure 10. Selecting the domain controllers policy to view

6. Select the **Default Domain Controllers Policy**, and click **OK**.



Select Group Policy Object

Group Policy Objects can be stored in the Active Directory or on a local computer.

Use the Browse button to select a Group Policy Object.

Group Policy Object:

Default Domain Controllers Policy

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

Figure 11. Closing the dialog box

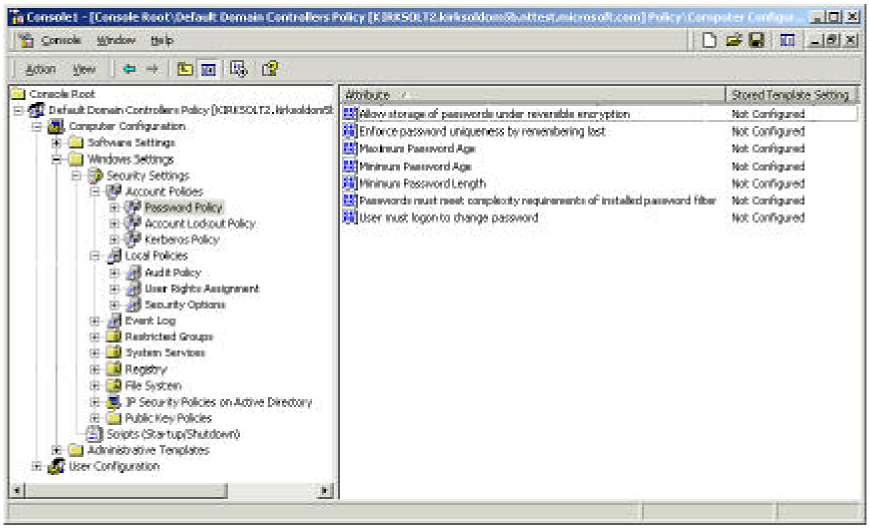
7. In the **Select Group Policy Object** dialog box, click **Finish**.

8. In the **Browse for a Group Policy Object** dialog box, click **OK**.

To review security policies in the default domain controllers GPO

1. In the **Default Domain Controllers** console, expand **Computer Configuration**, navigate to **Windows Settings**, then to **Security Settings**, and then to **Account Policies**.

2. Select **Password Policy**.

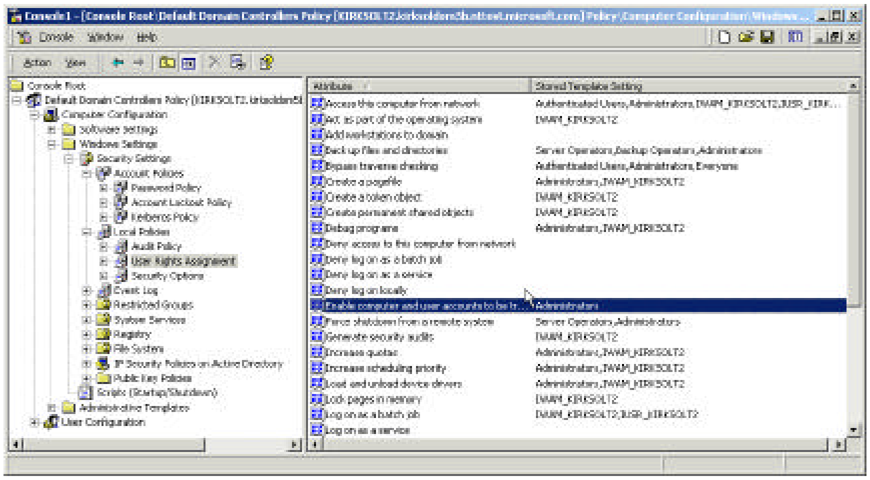


Attribute	Stored Template Setting
Allow storage of passwords under reversible encryption	Not Configured
Enforce password uniqueness by remembering last	Not Configured
Maximum Password Age	Not Configured
Minimum Password Age	Not Configured
Minimum Password Length	Not Configured
Passwords must meet complexity requirements of installed password filter	Not Configured
User must logon to change password	Not Configured

Figure 12. Viewing password policy

In the results pane, notice that a Password Policy is not defined in the default domain controllers GPO, because password policy is defined for the entire domain in the default domain GPO.

3. In the **Console**, navigate to **User Rights Assignments**, and select **User Rights Assignments**.



Attribute	Stored Template Setting
Access this computer from network	Authenticated Users,Administrators,IWAM_KIRKSOLT2,IUSR_KIRK...
Act as part of the operating system	IWAM_KIRKSOLT2
Add workstations to domain	
Back up files and directories	Server Operators,Backup Operators,Administrators
Bypass traverse checking	Authenticated Users,Administrators,Everyone
Create a pagefile	Administrators,IWAM_KIRKSOLT2
Create a token object	IWAM_KIRKSOLT2
Create permanent shared objects	IWAM_KIRKSOLT2
Debug programs	Administrators,IWAM_KIRKSOLT2
Deny access to this computer from network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Enable computer and user accounts to be tr...	Administrators
Force shutdown from a remote system	Server Operators,Administrators
Generate security audits	IWAM_KIRKSOLT2
Increase quotas	Administrators,IWAM_KIRKSOLT2
Increase scheduling priority	Administrators,IWAM_KIRKSOLT2
Load and unload device drivers	Administrators,IWAM_KIRKSOLT2
Lock pages in memory	IWAM_KIRKSOLT2
Log on as a batch job	IWAM_KIRKSOLT2,IUSR_KIRKSOLT2
Log on as a service	

Figure 13. Viewing user rights assignments

In the results pane, note that user rights are configured in the default domain controller GPO. As you saw in the previous section, user rights are not defined in the default domain GPO.

Summary

Account policies (password, lockout, Kerberos) are defined for the entire domain in the default domain GPO. Local policies (audit, user rights, and security options) for domain controllers are defined in the default domain controllers GPO. For domain controller's, settings defined in the default domain controllers GPO have higher precedence than settings defined in the default domain GPO. Thus, if you were to configure a user right (for example, *Add workstations to domain*) in the default domain GPO, it would have no impact on the domain controllers in that domain.

Notes The Account Policies security area receives special treatment in terms of how it takes effect on computers in the domain. All domain controllers in the domain receive their account policies from GPOs configured at the domain node *regardless of where the computer object for the DC is.* This ensures that consistent account policies are enforced for all domain accounts. All non-DC computers in the domain follow the normal GPO hierarchy in terms of getting account policies for the local accounts on those computers. By default, member workstations and servers enforce the account policy settings configured in the domain GPO for their local accounts, but if there is another GPO at lower scope that overrides the default settings, then those settings will take effect.

Allowing Administrators to Add Workstations to the Domain

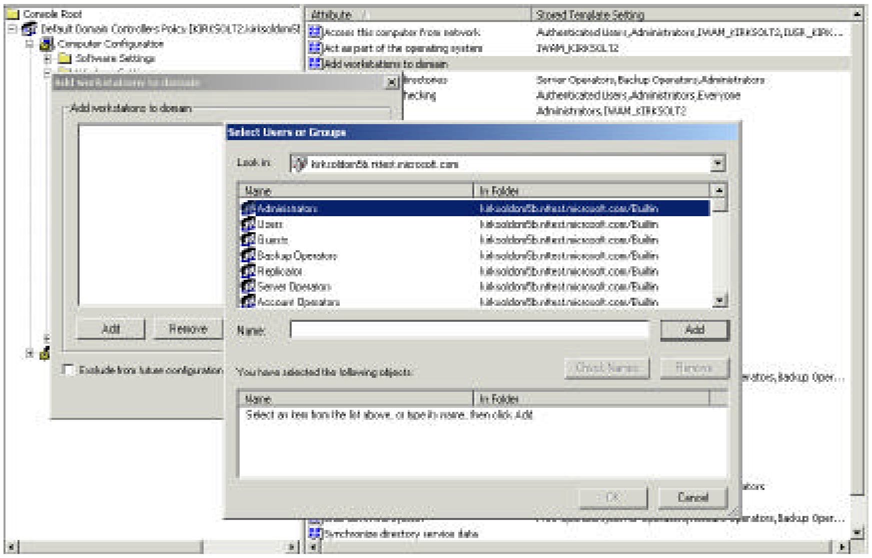
A machine account can be added to a domain before or during the domain join process. With Windows NT 4.0 or earlier, domain join privileges were granted through a specific user right (Add Workstation to Domain). With Windows 2000, a user should be given *create child* access on the computers container in the Active Directory for them to be able to add computers to the domain. For backward compatibility however, the *Add workstation to domain* user right still exists in Windows 2000. Users who have been granted this particular right can join a workstation to a domain even though they do not have create child access on the computers container.

As described above, this user right must be assigned in the default domain controller's GPO in order to have an effect on the domain controller machines which actually perform the access check for the domain join process. If the add workstation to domain user right was defined in the default domain GPO, then it would not have an effect on the domain controllers because by default, this privilege is defined in the default domain controller's GPO which has precedence over the default domain GPO. Changing the user right in the default domain GPO would thus only affect member workstations and servers where the user right has no meaning.

To add a workstation to a domain, use the console loaded with the Default Domain Controller GPO snap-in, which you opened in the previous scenario. The User Rights Assignment node should be selected.

To add a workstation to a domain

1. In the results pane, double-click the **Add workstation to domain** user right, and click **Add**.
2. In the **Select Users or Groups** dialog box, select **Administrators**, and click **Add**.



Console Root
Default Domain Controllers Policy [KIRKSOLT2.kirksoldom5b
Computer Configuration
Software Settings
Add workstations to domain
Add
Remove
□ Exclude from future configuration
Look in:
Add
Check Names
Remove
OK
Cancel

Select Users or Groups

Look in: kirksoldom5b.nttest.microsoft.com

Name	In Folder
Administrators	kirksoldom5b.nttest.microsoft.com/Builtin
Users	kirksoldom5b.nttest.microsoft.com/Builtin
Guests	kirksoldom5b.nttest.microsoft.com/Builtin
Backup Operators	kirksoldom5b.nttest.microsoft.com/Builtin
Replicator	kirksoldom5b.nttest.microsoft.com/Builtin
Server Operators	kirksoldom5b.nttest.microsoft.com/Builtin
Account Operators	kirksoldom5b.nttest.microsoft.com/Builtin

Name:

You have selected the following objects:

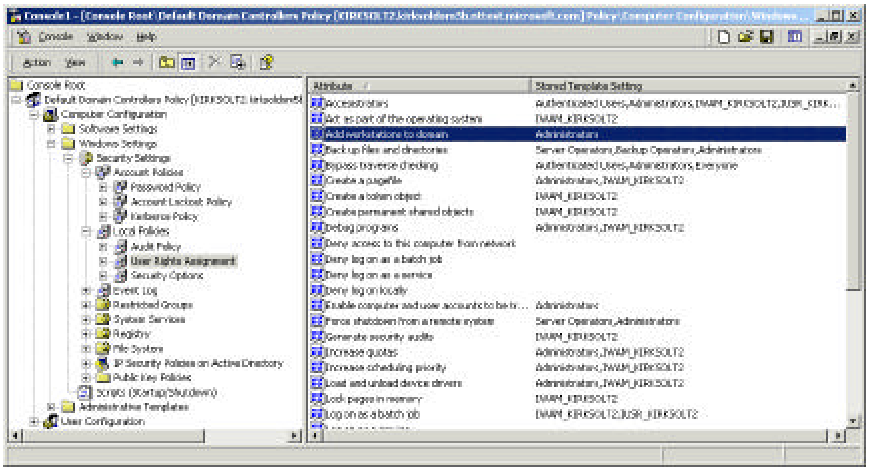
Name	In Folder
Select an item from the list above, or type its name, then click Add	

Attribute	Stored Template Setting
Access this computer from network	Authenticated Users,Administrators,IWAM_KIRKSOLT2,IUSR_KIRK...
Act as part of the operating system	IWAM_KIRKSOLT2
Add workstations to domain	
...irectories	Server Operators,Backup Operators,Administrators
...hecking	Authenticated Users,Administrators,Everyone
	Administrators,IWAM_KIRKSOLT2
Synchronize directory service data	

Figure 14. Adding the Administrators group

3. In the **Select Users or Groups** dialog box, click **OK**.

4. In the **Add Workstation to Domain** dialog box, click **OK**.



Console1 - [Console Root\Default Domain Controllers Policy [KIRKSOLT2.kirksoldom5b.nttest.microsoft.com] Policy\Computer Configuration\Windows ...

Attribute	Stored Template Setting
Access this computer from network	Authenticated Users,Administrators,IWAM_KIRKSOLT2,IUSR_KIRK...
Act as part of the operating system	IWAM_KIRKSOLT2
Add workstations to domain	Administrators
Back up files and directories	Server Operators,Backup Operators,Administrators
Bypass traverse checking	Authenticated Users,Administrators,Everyone
Create a pagefile	Administrators,IWAM_KIRKSOLT2
Create a token object	IWAM_KIRKSOLT2
Create permanent shared objects	IWAM_KIRKSOLT2
Debug programs	Administrators,IWAM_KIRKSOLT2
Deny access to this computer from network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Enable computer and user accounts to be tr...	Administrators
Force shutdown from a remote system	Server Operators,Administrators
Generate security audits	IWAM_KIRKSOLT2
Increase quotas	Administrators,IWAM_KIRKSOLT2
Increase scheduling priority	Administrators,IWAM_KIRKSOLT2
Load and unload device drivers	Administrators,IWAM_KIRKSOLT2
Lock pages in memory	IWAM_KIRKSOLT2
Log on as a batch job	IWAM_KIRKSOLT2,IUSR_KIRKSOLT2

Figure 15. Viewing the results of assigning a user right to administrators

Enabling Auditing on All Domain Controllers

Using the same console as above, you can modify the audit policy for domain controllers.

To enable auditing

1. In the scope pane, select **Audit Policy**.

2. In the result pane, double-click **Audit Directory Service Access**.

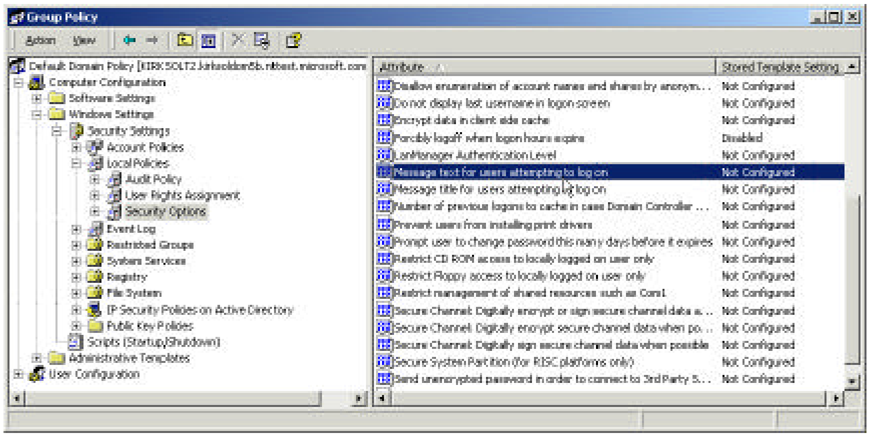
3. Select **Audit Failed Attempts,** and click **OK**. The settings should be updated in the result pane.
4. Close the console loaded with the **Default Domain Controller GPO** snap-in.
5. When prompted to save console settings, click **No**.

Establishing a Logon Message for All Machines in the Domain

To establish a logon message for all the computers in a domain, you'll use the Active Directory Users and Computers snap-in described you opened in the first scenario of this walkthrough, "Viewing Default Domain Security Policies."

To establish a logon message

1. In the **Group Policy Editor**, which is focused on the Default Domain Policy, expand **Computer Configuration**, then **Windows Settings**, navigate to **Security Settings**, then to **Local Policies**, and select **Security Options**.



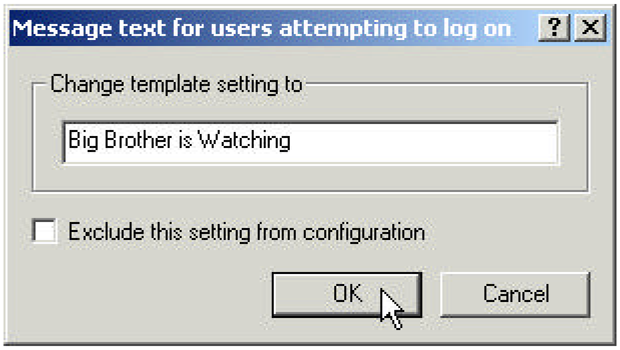
Attribute	Stored Template Setting
Disallow enumeration of account names and shares by anonym...	Not Configured
Do not display last username in logon screen	Not Configured
Encrypt data in client side cache	Not Configured
Forcibly logoff when logon hours expire	Disabled
LanManager Authentication Level	Not Configured
Message text for users attempting to log on	Not Configured
Message title for users attempting to log on	Not Configured
Number of previous logons to cache in case Domain Controller ...	Not Configured
Prevent users from installing print drivers	Not Configured
Prompt user to change password this many days before it expires	Not Configured
Restrict CD ROM access to locally logged on user only	Not Configured
Restrict Floppy access to locally logged on user only	Not Configured
Restrict management of shared resources such as Com1	Not Configured
Secure Channel: Digitally encrypt or sign secure channel data a...	Not Configured
Secure Channel: Digitally encrypt secure channel data when po...	Not Configured
Secure Channel: Digitally sign secure channel data when possible	Not Configured
Secure System Partition (for RISC platforms only)	Not Configured
Send unencrypted password in order to connect to 3rd Party S...	Not Configured

Figure 16. Selecting security options

2. In the results pane, double-click **Message text for users attempting to log on**.
3. Click to clear the **Exclude this setting from configuration** check box.
4. Type a message that you want a user to see when he or she logs on to any computer in the domain. In this example, type

   Big Brother is Watching

   and click **OK**. The setting should be updated in the results pane.



Message text for users attempting to log on

Change template setting to

Big Brother is Watching

□ Exclude this setting from configuration

Figure 17. Creating a message text

5. Close the **Group Policy Editor**.
6. Close the domain **Properties** page.
7. Close the **Active Directory Users and Computers** snap-in.

Since this security setting is associated with the default domain GPO, it applies to all computers in the domain. This setting will override any local policies (defined on individual computers) that specify this security parameter, but will not override any OU policies that specify this value.

Note When you make a change to a GPO, the change is saved immediately in the GPO's storage. However, the change is not implemented on target machines until policy propagation is triggered on the target computer. By default, policy is refreshed on domain controllers every five minutes. If the GPO has been replicated to a domain controller, the policy change is implemented at the refresh time. On workstations and member servers, policy is refreshed every 60-90 minutes. During a refresh on workstations and member servers, updated GPOs are automatically downloaded (not replicated). You can view the effective policy on a domain controller by viewing the domain controller's local policy.

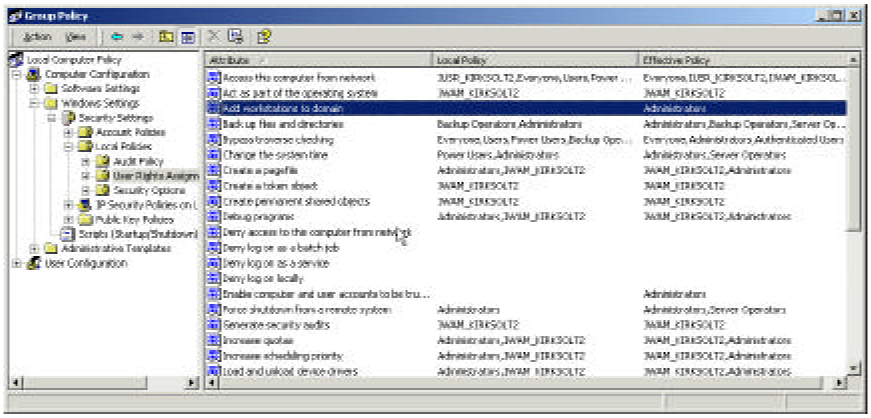
Viewing a Domain Controller's Effective Security Policy

To view domain controller's effective security policy

1. On the **Start** menu, click **Run**. In the Open text box, type:

   GPEdit.msc

   and then click **OK**.
2. In the Group Policy Editor's scope pane, expand **Computer Configuration**, navigate to **Windows Settings**, to **Security Settings,** then to **Local Policies**.
3. Select **User Rights Assignment**.

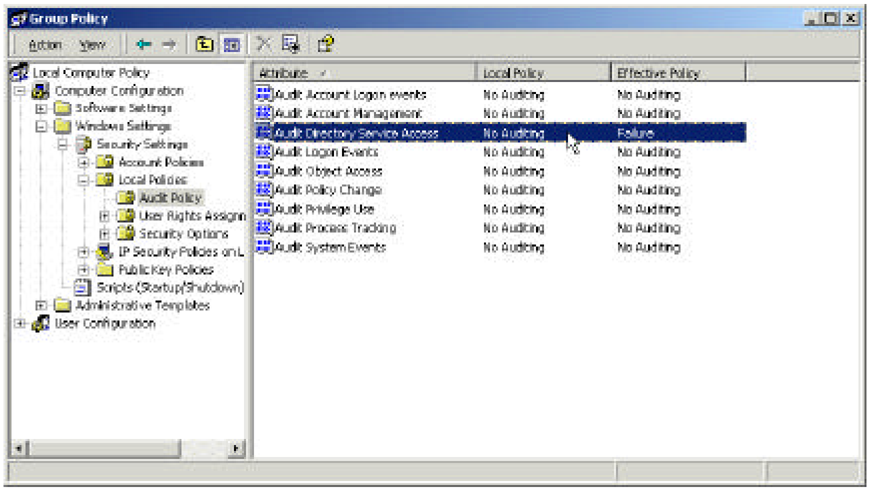


Attribute	Local Policy	Effective Policy
Access this computer from network	IUSR_KIRKSOLT2,Everyone,Users,Power ...	Everyone,IUSR_KIRKSOLT2,IWAM_KIRKSOL...
Act as part of the operating system	IWAM_KIRKSOLT2	IWAM_KIRKSOLT2
Add workstations to domain		Administrators
Back up files and directories	Backup Operators,Administrators	Administrators,Backup Operators,Server Op...
Bypass traverse checking	Everyone,Users,Power Users,Backup Ope...	Everyone,Administrators,Authenticated Users
Change the system time	Power Users,Administrators	Administrators,Server Operators
Create a pagefile	Administrators,IWAM_KIRKSOLT2	IWAM_KIRKSOLT2,Administrators
Create a token object	IWAM_KIRKSOLT2	IWAM_KIRKSOLT2
Create permanent shared objects	IWAM_KIRKSOLT2	IWAM_KIRKSOLT2
Debug programs	Administrators,IWAM_KIRKSOLT2	IWAM_KIRKSOLT2,Administrators
Deny access to this computer from network		
Deny log on as a batch job		
Deny log on as a service		
Deny log on locally		
Enable computer and user accounts to be tru...		Administrators
Force shutdown from a remote system	Administrators	Administrators,Server Operators
Generate security audits	IWAM_KIRKSOLT2	IWAM_KIRKSOLT2
Increase quotas	Administrators,IWAM_KIRKSOLT2	IWAM_KIRKSOLT2,Administrators
Increase scheduling priority	Administrators,IWAM_KIRKSOLT2	IWAM_KIRKSOLT2,Administrators
Load and unload device drivers	Administrators,IWAM_KIRKSOLT2	IWAM_KIRKSOLT2,Administrators

Figure 18. Viewing the domain controller's Local Policy

Now you can view the domain controller's local computer policy. Notice that the effective policy grants administrators the right to Add workstations to the domain while the local policy grants this privilege to no one. The local policy is overridden by the default domain controllers policy previously configured.

4. Select **Audit Policy**.

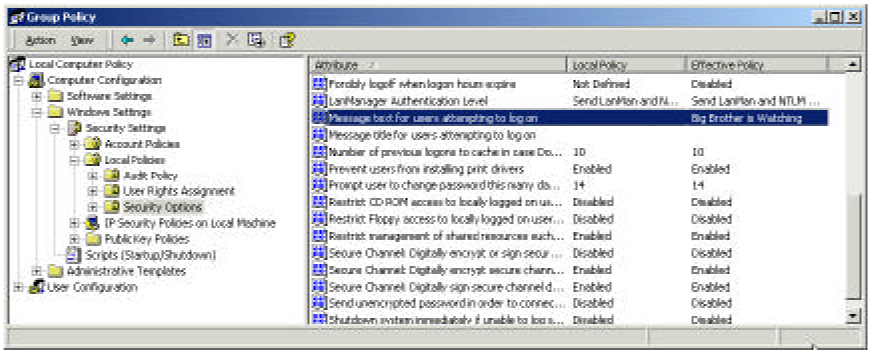


Attribute	Local Policy	Effective Policy
Audit Account Logon events	No Auditing	No Auditing
Audit Account Management	No Auditing	No Auditing
Audit Directory Service Access	No Auditing	Failure
Audit Logon Events	No Auditing	No Auditing
Audit Object Access	No Auditing	No Auditing
Audit Policy Change	No Auditing	No Auditing
Audit Privilege Use	No Auditing	No Auditing
Audit Process Tracking	No Auditing	No Auditing
Audit System Events	No Auditing	No Auditing

Figure 19. Viewing the Audit Policy change

Similarly, the audit change made to the default domain controller GPO is also reflected in the domain controller's effective policy.

5. Select **Security Options**.



Attribute	Local Policy	Effective Policy
Forcibly logoff when logon hours expire	Not Defined	Disabled
LanManager Authentication Level	Send LanMan and N...	Send LanMan and NTLM ...
Message text for users attempting to log on		Big Brother is Watching
Message title for users attempting to log on		
Number of previous logons to cache in case Do...	10	10
Prevent users from installing print drivers	Enabled	Enabled
Prompt user to change password this many da...	14	14
Restrict CD ROM access to locally logged on us...	Disabled	Disabled
Restrict Floppy access to locally logged on user...	Disabled	Disabled
Restrict management of shared resources such...	Enabled	Enabled
Secure Channel: Digitally encrypt or sign secur ...	Disabled	Disabled
Secure Channel: Digitally encrypt secure chann...	Enabled	Enabled
Secure Channel: Digitally sign secure channel d...	Enabled	Enabled
Send unencrypted password in order to connec...	Disabled	Disabled
Shutdown system immediately if unable to log s...	Disabled	Disabled

Figure 20. Message text for users as part of the default domain policy

Here you can see the message text coming from the default domain policy (not the default domain controllers policy)

6. Close the **Group Policy\Local Computer Policy** snap-in.
7. When prompted to save console settings, click **No**.

Notes

As you saw when auditing object access in previous beta releases of Windows 2000, enabling auditing policy for directory access is only part of the work associated with setting up and starting auditing. You must also configure auditing on the various directory objects that must be audited, and you might have to adjust the defaults. For example, the default behavior is to start auditing *write* events done to the directory (both failed and successful), but not reads. This is based on the assumption that most access to the directory will be *read* attempts, and that these are typically legitimate.

Also, note that all DCs are placed in the Domain Controllers OU by default. This implies that by default, all DCs will show consistent local policies (audit, user rights, and security options). However, if you move a DC out of this OU, that DC will enforce the policy based on its new container. As described earlier, this is different from DC behavior with respect to account policies (password, lockout, and Kerberos), where domain controllers implement the policy configured at the domain level.

This means that different domain controllers in the same domain (but different OUs) can have different local policies (audit, user rights, and security options). For example, a DC in New York might have different backup operators than a DC in London.

Enforcing a Remote Access Security Policy

In this walkthrough, you will enforce a security policy that states that the Windows 2000 Remote Access Service (RAS) should run only on designated RAS Servers and on no other computers in the enterprise. Further, it will specify that only Enterprise Administrators will have control over the RAS Service on the RAS Servers.

To accomplish this task, you will create two new GPOs:

- **Disable RAS**—a GPO that will disable the RAS service. This policy will be assigned at the domain node so that it affects every computer in the domain.
- **Enable RAS**—a GPO that autostarts RAS and sets security on the service so that only the Administrators group (and local system) have access to the service. This policy will be assigned to the RAS Servers OU so that it will override the Disable RAS GPO defined at the domain level. Thus, only computers in the RAS Servers OU can (and must) run RAS.

Create the RAS Servers OU

To create the RAS Server organizational unit, you must first load the Active Directory Users and Computers snap-in.

To create the RAS Servers OU

1. On the **Start** menu, point to **Programs**, then point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

2. **In the snap-in**, expand your **domain** folder to reveal the default containers. Note that there is a Domain Controllers OU within the domain.

3. Right-click your domain name, and then select **New**, **Organizational Unit**.

4. For the name of the OU, type

   RAS Servers

   and click **OK**.

5. Close the **Active Directory Users and Computers** snap-in.

Create a New Domain-level GPO to DisableRAS

To create a new domain-level GPO to disable RAS, you must first load the Group Policy snap-in.

To load the snap-in

1. On the **Start** menu, point to **Run**. In the **Open** text box, type:

   mmc /s

2. Click **Console**, and then click **Add/Remove Snap-in**.

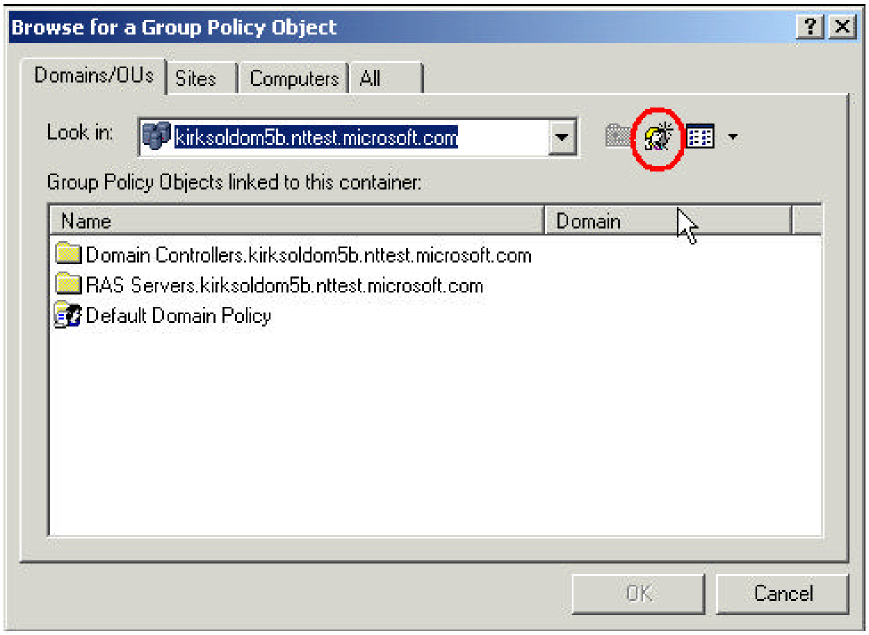
3. Click **Add**.

4. Select **Group Policy** from the list, and click **Add**. The **Select Group Policy Object** dialog box is displayed.

5. Click **Browse**. The **Browse for a Group Policy Object** dialog box is displayed.

   Notice that the RAS Servers OU is listed as a possible location where you can link the GPO. However, the Disable RAS GPO belongs with the domain.

6. Click the **Create New GPO** button.



Look in: kirksoldom5b.nttest.microsoft.com

Group Policy Objects linked to this container:

Name	Domain
Domain Controllers.kirksoldom5b.nttest.microsoft.com	
RAS Servers.kirksoldom5b.nttest.microsoft.com	
Default Domain Policy	

Figure 21. The Create New GPO button (circled)

7. Modify the default name of the new GPO. Call it **DisableRAS** and click **OK**.

8. Click **Finish**.

9. Close the **Add Standalone Snap-in** dialog box.

10. Click **OK** to close the **Add/Remove Snap-in** dialog box.

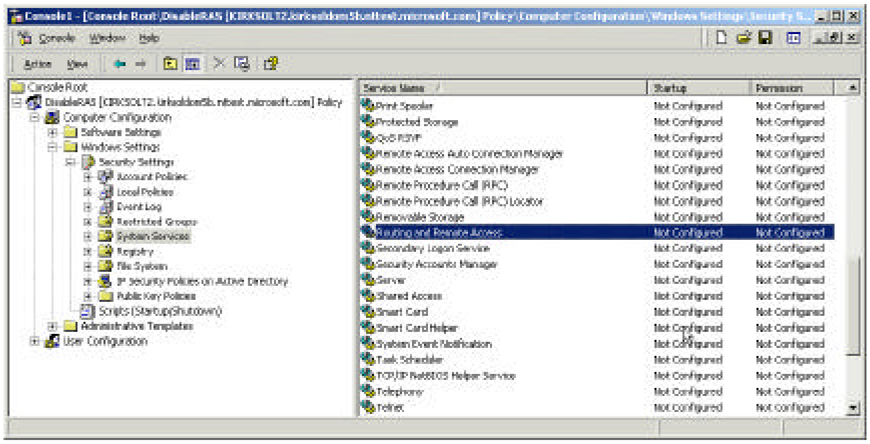
    There is a bug in Windows 2000 Beta 3 that prevents the security settings extension to Group Policy from displaying when a newly created GPO is expanded. To work around this problem, you must close the Group Policy snap-in and reload the newly created Disable RAS GPO, as follows:

    1. Close the Group Policy Snap-in.
    2. When prompted to save the console settings, click **No**.
    3. Redo steps 1 to 6 above, and then select the **DisableRAS** GPO rather than creating a new one.

    Now you have the Group Policy Editor focused on the newly created GPO.

11. In the scope pane of the console, expand **DisableRAS**, and navigate to **Computer Configuration**, to **Windows Settings**, and then to **Security Settings**.

12. Select **System Services**.


Console1 - [Console Root\DisableRAS [KIRKSOLT2.kirkseldom5b.nttest.microsoft.com] Policy\Computer Configuration\Windows Settings\Security S...
Console
Window
Help
Action
View
Console Root
DisableRAS [KIRKSOLT2.kirkseldom5b.nttest.microsoft.com] Policy
Computer Configuration
Software Settings
Windows Settings
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
IP Security Policies on Active Directory
Public Key Policies
Scripts (Startup/Shutdown)
Administrative Templates
User Configuration

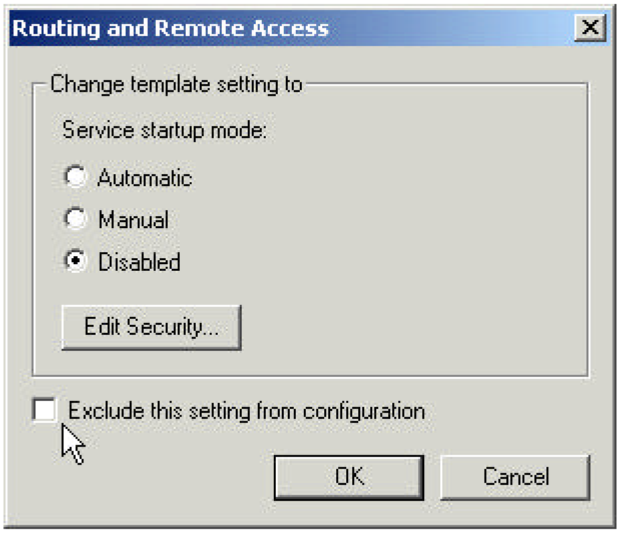
Service Name	Startup	Permission
Print Spooler	Not Configured	Not Configured
Protected Storage	Not Configured	Not Configured
QoS RSVP	Not Configured	Not Configured
Remote Access Auto Connection Manager	Not Configured	Not Configured
Remote Access Connection Manager	Not Configured	Not Configured
Remote Procedure Call (RPC)	Not Configured	Not Configured
Remote Procedure Call (RPC) Locator	Not Configured	Not Configured
Removable Storage	Not Configured	Not Configured
Routing and Remote Access	Not Configured	Not Configured
Secondary Logon Service	Not Configured	Not Configured
Security Accounts Manager	Not Configured	Not Configured
Server	Not Configured	Not Configured
Shared Access	Not Configured	Not Configured
Smart Card	Not Configured	Not Configured
Smart Card Helper	Not Configured	Not Configured
System Event Notification	Not Configured	Not Configured
Task Scheduler	Not Configured	Not Configured
TCP/IP NetBIOS Helper Service	Not Configured	Not Configured
Telephony	Not Configured	Not Configured
Telnet	Not Configured	Not Configured

Figure 22. Selecting a system service

13. In the list of service names, double-click **Routing and Remote Access**.

14. Click to clear the **Exclude this setting from configuration** check box.

15. Select **Disabled**, and click **OK**.



Change template setting to

Service startup mode:

○ Automatic

○ Manual

● Disabled

□ Exclude this setting from configuration

Figure 23. Disabling RAS

16. Close the **Group Policy** snap-in.

17. When prompted to save the console settings, click **No**.

You have now established a policy to disable RAS on all computers in the domain.

Create a Security Template to Hold EnableRAS Policy

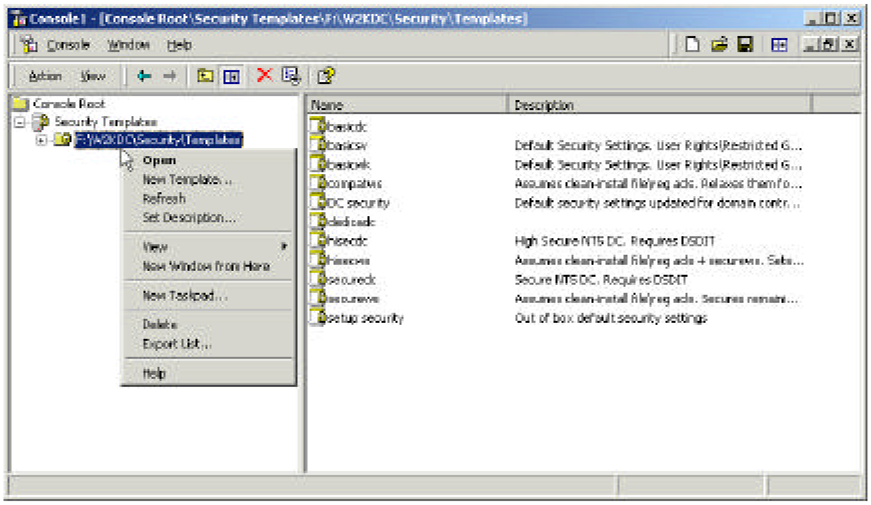
It is possible to create security policies in text files and then import them into GPOs. To create the EnableRAS policy, you must first create a security template to hold the EnableRAS policy.

To create a security template

1. On the **Start** menu, click **Run**. In the **Open** text box, type:

   mmc /s

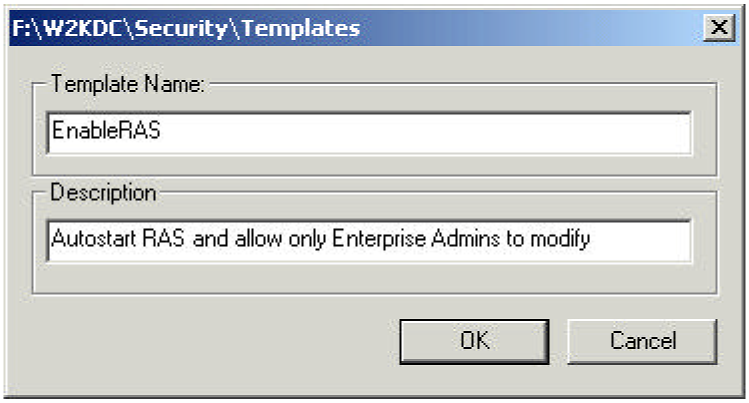
2. From the **Console** menu, select **Add/Remove Snap-in**.
3. Click **Add**.
4. From the list of available standalone snap-ins, select **Security Templates** and click **Add**.
5. Click **Close**, and then **OK**.
6. Expand **the Security Templates node**.
7. Select **%windir%\security\templates**, the default security templates path.
8. Right-click the **security templates** path, and then select **New Template**.



Name	Description
basicdc	
basicsv	Default Security Settings. User Rights\Restricted G...
basicwk	Default Security Settings. User Rights\Restricted G...
compatws	Assumes clean-install file\reg acls. Relaxes them fo...
DC security	Default security settings updated for domain contr...
dedicadc	
hisecdc	High Secure NT5 DC. Requires DSDIT
hisecws	Assumes clean-install file\reg acls + securews. Sets...
securedc	Secure NT5 DC. Requires DSDIT
securews	Assumes clean-install file\reg acls. Secures remaini...
setup security	Out of box default security settings

Figure 24. Creating a new template

9. Type **EnableRAS** in the **Template Name** box, and type a description of the security policy in the **Description** box, and click **OK**.

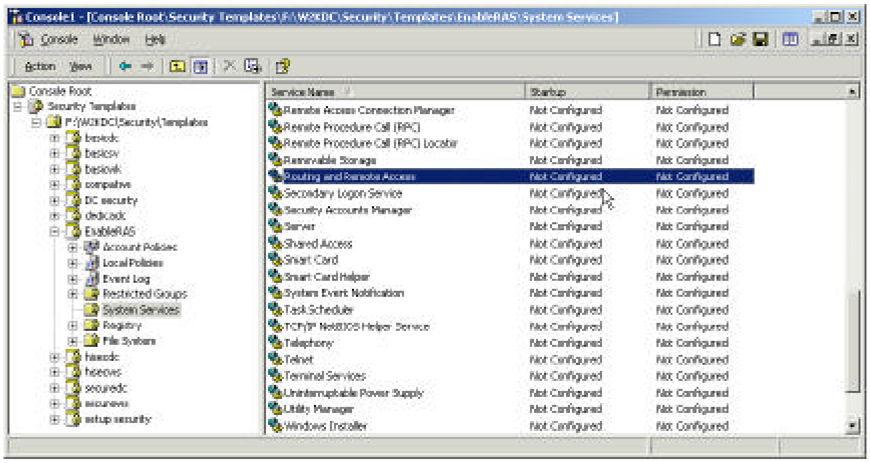


Template Name: EnableRAS

Description: Autostart RAS and allow only Enterprise Admins to modify

Figure 25. Naming and describing the new template

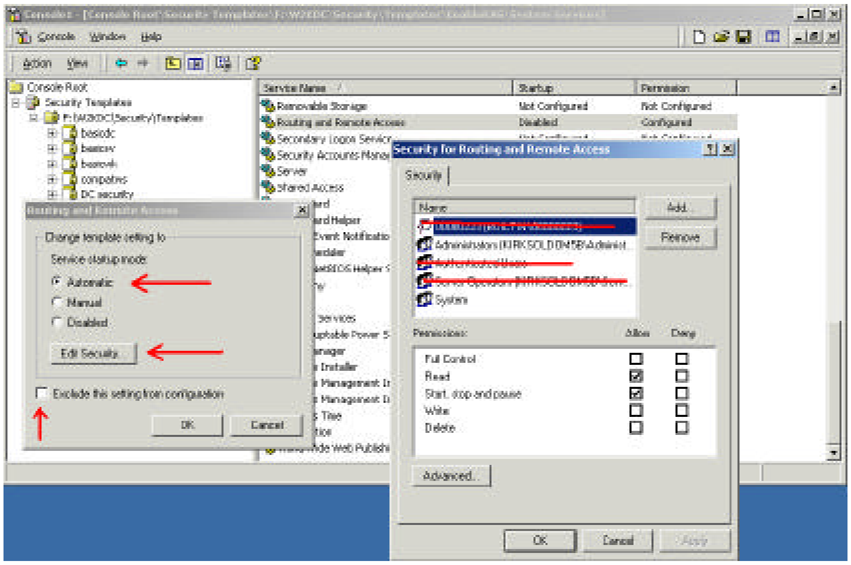
10. Expand **%windir%\security\templates**, and navigate to **EnableRAS**.
11. Expand **EnableRAS**, and select **System Services**.



Service Name	Startup	Permission
Remote Access Connection Manager	Not Configured	Not Configured
Remote Procedure Call (RPC)	Not Configured	Not Configured
Remote Procedure Call (RPC) Locator	Not Configured	Not Configured
Removable Storage	Not Configured	Not Configured
Routing and Remote Access	Not Configured	Not Configured
Secondary Logon Service	Not Configured	Not Configured
Security Accounts Manager	Not Configured	Not Configured
Server	Not Configured	Not Configured
Shared Access	Not Configured	Not Configured
Smart Card	Not Configured	Not Configured
Smart Card Helper	Not Configured	Not Configured
System Event Notification	Not Configured	Not Configured
Task Scheduler	Not Configured	Not Configured
TCP/IP NetBIOS Helper Service	Not Configured	Not Configured
Telephony	Not Configured	Not Configured
Telnet	Not Configured	Not Configured
Terminal Services	Not Configured	Not Configured
Uninterruptable Power Supply	Not Configured	Not Configured
Utility Manager	Not Configured	Not Configured
Windows Installer	Not Configured	Not Configured

Figure 26. Locating the Routing and Remote Access service

12. In the result pane, double-click **Routing and Remote Access**.
13. Clear the **Exclude this setting from configuration** checkbox, and select Automatic for the service startup mode.
14. Click **Edit Security**. The **Service Access Control List Editor** is displayed.



Service Name	Startup	Permission
Removable Storage	Not Configured	Not Configured
Routing and Remote Access	Disabled	Configured

Routing and Remote Access

Change template setting to

Service startup mode

● Automatic

○ Manual

○ Disabled

Edit Security...

□ Exclude this setting from configuration

OK Cancel

Security for Routing and Remote Access

Name

~~[illegible]~~

Administrators (KIRKSOLD DM5B\Administ...

~~Authenticated Users~~

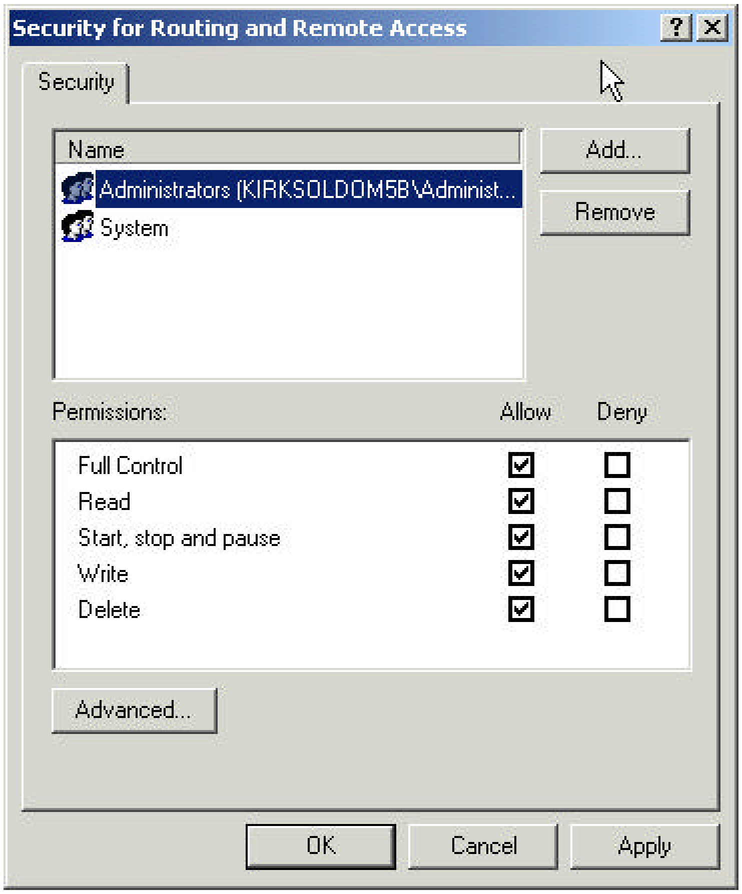
~~Server Operators (KIRKSOLD DM5B\Serv...~~

System

Permissions:	Allow	Deny
Full Control	□	□
Read	☑	□
Start, stop and pause	☑	□
Write	□	□
Delete	□	□

Figure 27. Specifying the service start up mode and using the Service Access Control Editor (ACL)

15. In the **Service Access Control List Editor**, select all security principals **except for Administrators and System**, and click **Remove**.



Name

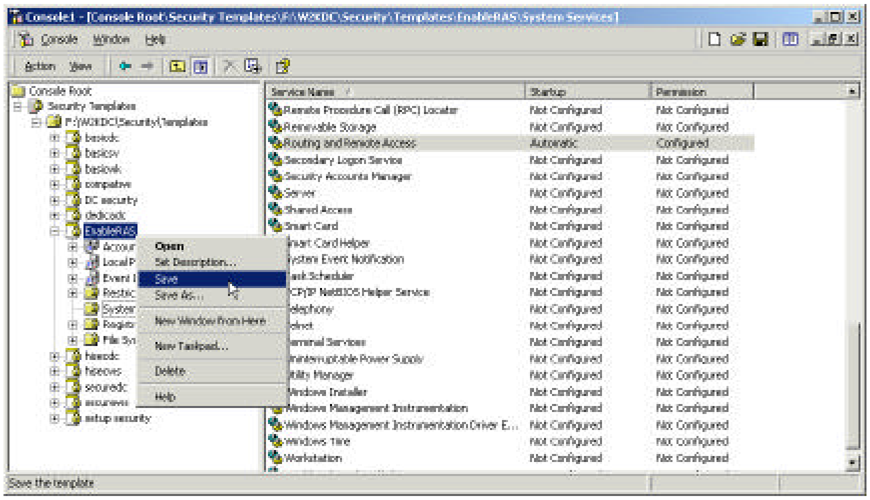
Administrators (KIRKSOLDOM5B\Administ...

System

Permissions:	Allow	Deny
Full Control	☑	□
Read	☑	□
Start, stop and pause	☑	□
Write	☑	□
Delete	☑	□

Figure 28. Using the ACL Editor to specify permissions

16. Click **OK** to close the **Service ACL Editor**.
17. Click **OK** to close the **Routing and Remote Access Startup Mode** dialog box.
18. Right-click the **EnableRAS** template, and then click **Save**.



Service Name	Startup	Permission
Remote Procedure Call (RPC) Locator	Not Configured	Not Configured
Removable Storage	Not Configured	Not Configured
Routing and Remote Access	Automatic	Configured
Secondary Logon Service	Not Configured	Not Configured
Security Accounts Manager	Not Configured	Not Configured
Server	Not Configured	Not Configured
Shared Access	Not Configured	Not Configured
Smart Card	Not Configured	Not Configured
mart Card Helper	Not Configured	Not Configured
ystem Event Notification	Not Configured	Not Configured
ask Scheduler	Not Configured	Not Configured
CP/IP NetBIOS Helper Service	Not Configured	Not Configured
elephony	Not Configured	Not Configured
elnet	Not Configured	Not Configured
erminal Services	Not Configured	Not Configured
ninterruptable Power Supply	Not Configured	Not Configured
tility Manager	Not Configured	Not Configured
indows Installer	Not Configured	Not Configured
indows Management Instrumentation	Not Configured	Not Configured
Windows Management Instrumentation Driver E...	Not Configured	Not Configured
Windows Time	Not Configured	Not Configured
Workstation	Not Configured	Not Configured

Figure 29. Saving the new security settings

19. Close the **Security Templates** snap-in, and when prompted to save the console settings, click **No**.

20. When prompted to save the **EnableRAS** template file, click **OK**.

The security settings for the EnableRAS policy are now saved in the EnableRAS security template. Next, you will import these settings into the new EnableRAS GPO.

Create the EnableRAS GPO for the RAS Servers OU

To create EnableRAS GPO

1. On the Start menu, point to **Programs**, then point to **Administrative Tools**, and click **Active Directory Users and Computers**.

2. In the scope pane, expand your **domain** folder.

3. Select the **RAS Servers** OU, right-click it, and then click **Properties**. The RAS Servers Properties dialog box is displayed.

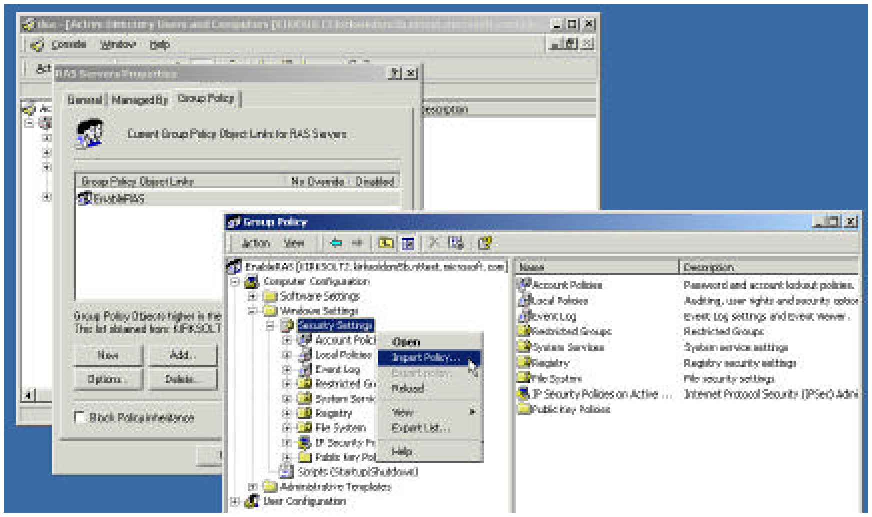
4. Select the **Group Policy** tab, and click **New**.

5. Type **EnableRAS** for the name of the new GPO, and then click **Edit**.

6. In the Group Policy snap-in, expand **Computer Configuration**, to **Windows Settings**, and select **Security Settings**.

   Now you can import the previously configured EnableRAS policy.

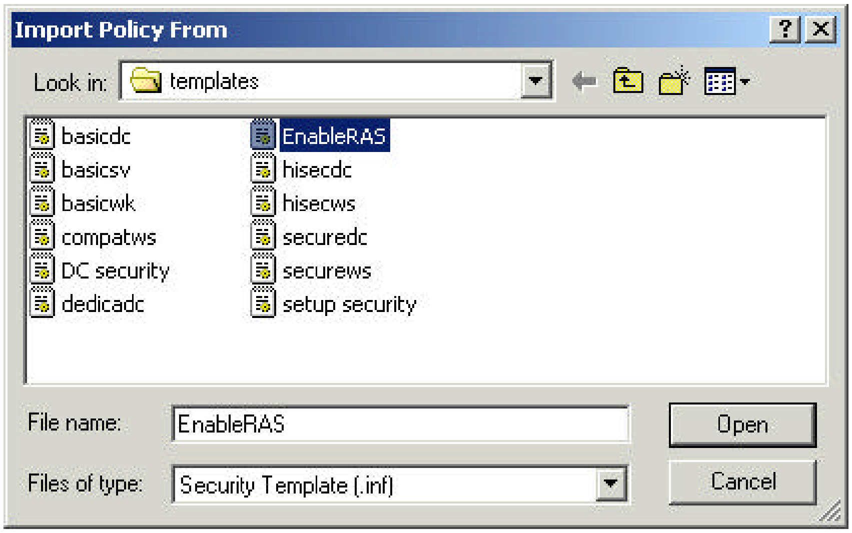
7. Right-click **Security Settings**, then select **Import Policy**.



Name	Description
Account Policies	Password and account lockout policies.
Local Policies	Auditing, user rights and security option
Event Log	Event Log settings and Event Viewer.
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
IP Security Policies on Active ...	Internet Protocol Security (IPSec) Admi
Public Key Policies	

Figure 30. Importing the new EnableRAS policy

8. Select the **EnableRAS.inf** file that you previously created, and click **Open**.



Look in: templates

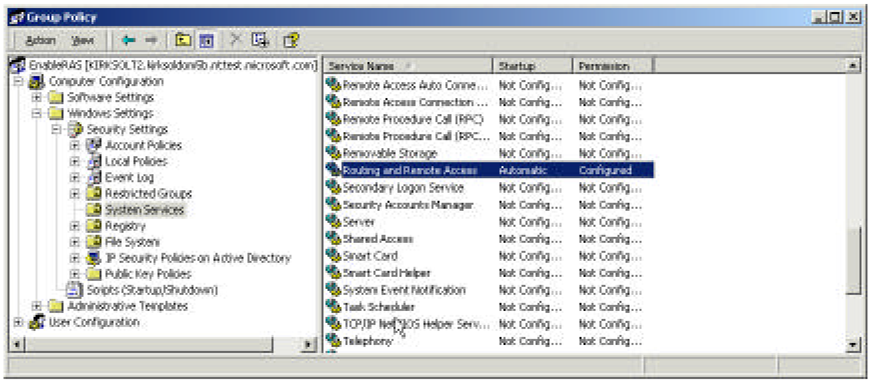
basicdc
basicsv
basicwk
compatws
DC security
dedicadc
EnableRAS
hisecdc
hisecws
securedc
securews
setup security

File name: EnableRAS

Files of type: Security Template (.inf)

Figure 31. Security templates are stored as INF files

9. Select **System Services** for the EnableRAS GPO.



Service Name	Startup	Permission
Remote Access Auto Conne…	Not Config…	Not Config…
Remote Access Connection …	Not Config…	Not Config…
Remote Procedure Call (RPC)	Not Config…	Not Config…
Remote Procedure Call (RPC…	Not Config…	Not Config…
Removable Storage	Not Config…	Not Config…
Routing and Remote Access	Automatic	Configured
Secondary Logon Service	Not Config…	Not Config…
Security Accounts Manager	Not Config…	Not Config…
Server	Not Config…	Not Config…
Shared Access	Not Config…	Not Config…
Smart Card	Not Config…	Not Config…
Smart Card Helper	Not Config…	Not Config…
System Event Notification	Not Config…	Not Config…
Task Scheduler	Not Config…	Not Config…
TCP/IP NetBIOS Helper Serv…	Not Config…	Not Config…
Telephony	Not Config…	Not Config…

Figure 32. Viewing the settings in EnableRAS GPO

Notice that the settings defined in the Security Template have been imported into the EnableRAS GPO.

10. Close the **Group Policy** snap-in, close the **RAS Servers Properties** dialog box, and then close the **Active Directory Users and Computers** snap-in.

RAS servers that are moved into the RAS Servers OU will not automatically start the RAS Service. Only Administrators will be able to control the RAS Service on these servers. Finally, no other computer in the domain can run the RAS Service.

FOR MORE INFORMATION

For the latest information on Windows 2000, visit our Web site at http://www.microsoft.com/windows/server and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at http://ntbeta.microsoft.com

Feedback

Please help us make the product better by sending feedback regarding the Security Configuration Tool Set, default security settings and security templates to scefeed@microsoft.com. Note that this is not a support alias.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.